# 准备：

1 MAME模拟器或Arcade模拟器

2 Notepad++及比较插件 [已附件插件 notepad++自行下载]

若是不会基本的调试器操作，先去看我的这个帖子

<https://www.ppxclub.com/forum.php?mod=viewthread&tid=693442>

感谢 bleempan 前辈的思路指导

思路是对比击中与未击中的汇编指令，

所以准备好诸如锁定敌方坐标或是敌方不可动的作弊功能，

以及设置好暂停与帧进的快捷键，

(游戏内按Tab键，输入设置全局 - 用户界面 - 暂停 / 暂停-单步，自己设置快捷键，

英文版为 Input General - User Interface - Pause / Pause-Single Step )

**需要注意的是，尽量让trace帧进的情景相同，让差异只存在于击中与未击中，**

**并且让每一次帧进发生的动作都是一样，这样trace出来的无用指令地址就会极大的减少**

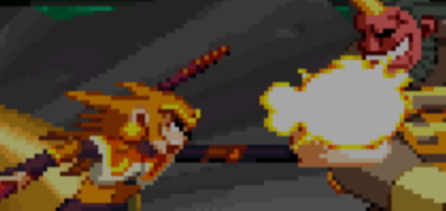
准备好后用模拟器带调试器进入要修改的游戏，

我拿西游释厄传2举栗，

开启”敌方不可动”后，选择”孙悟空”进入”挑战魔王”模式，



攻击的瞬间暂停，然后帧进，会发现掌风出现后再次帧进就会攻击到敌方，



但若是只导出这一帧的指令，是没有关键跳转的，

所以站一个远一点攻击不到敌方的地方，攻击瞬间暂停，



大概这个姿势就够了，很明显这样是打不到的，现在导出未攻击到的指令，

在调试器里键入 trace 1.txt

(trace为跟踪记录指令，1.txt为保存到的文件名，记录到的所有指令都会保存到根目录的1.txt，但需要注意的是如神剑伏魔录等游戏地址是存在于非maincpu 的CPU，

需要按F6切换到指定CPU才能导出对应的汇编地址，如神剑伏魔录要切换到prot，

否则无法找到关键跳转)

然后开始帧进，切记这时候也就是trace开启状态不要解除游戏暂停，

不然会导出几百M的指令，我们需要的只是帧进，导出我们需要的指令就行，

帧进大概10次，然后键入 trace off

(意为关闭trace跟踪记录)

先不管这次保存的文件，来到敌方面前，



依然是攻击瞬间暂停，然后这个姿势时键入 trace 2.txt

刚才保存的是1.txt，名字可以自己取，只要分得清

然后帧进大概10次，

键入 trace off



两个文件都保存到了模拟器根目录，

1.txt为未击中，2.txt为击中

对比指令有了，还需要一个切入点，也就是击中扣血指令，

简单说就是打中了才会有扣血指令，而这肯定会有个判断，

调试器里键入 ci sw 二字节初始化，打一下敌方就 cn - 一次，

重复筛选，然后依次测试找到正确地址，我找到的是2005474C，

(但如神剑伏魔录等游戏地址是存在于非maincpu的CPU，这一点和之前提到的一样，

如神剑伏魔录，初始化搜索要切换到prot CPU执行，其次初始化也要加参数，

如搜索时间，变化区间在0~99，那就这样初始化 ci sb,0x18000000,0x200000,2

若是看不懂，把我之前发的MAME调试器教程多看几遍)

键入 wp 2005474C,1,w对其下写入监视断点，

打一下敌方就会断下来，唯一一条，



1001BAEA即为扣血指令地址，记录下

剩下的就是对比了，目力对比是很麻烦的，

所以就需要借助工具，



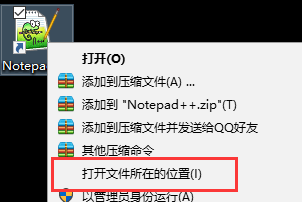
Notepad++是一款很好用的记事本工具，支持插件，

X64为64位，x86为32位，优先装64位

一直下一步安装即可，

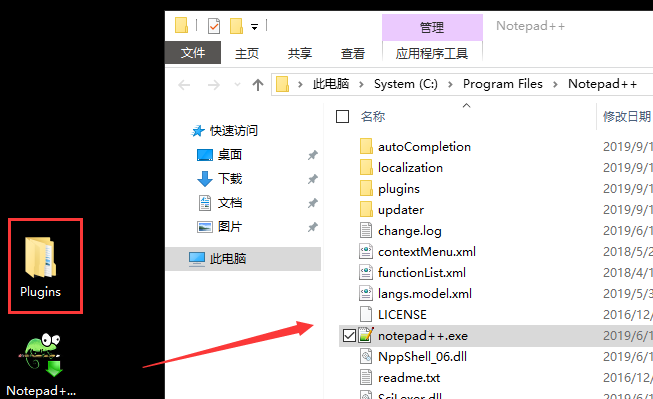


意为创建桌面快捷方式，勾选上，方便下一步放插件，

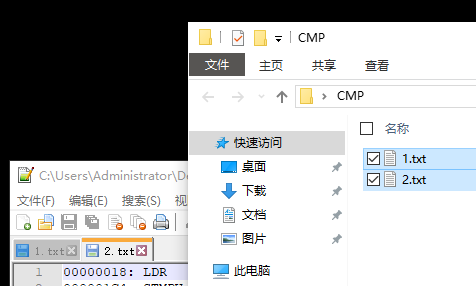


安装完成后若是打开了Notepad++，关闭，

然后在桌面图标上右键，打开文件所在位置，

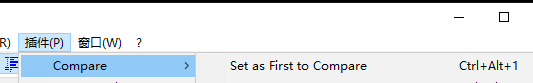


直接把Plugins文件夹拖入Notepad++安装目录，再打开Notepad++



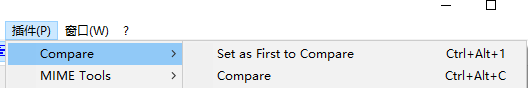
选中刚才导出的两个文件，将其拖入Notepad++

2.txt是击中指令，优先对比，可以按Ctrl+Alt+1或



设置为首要对比项，

再选择1.txt标签按Ctrl+Alt+C或



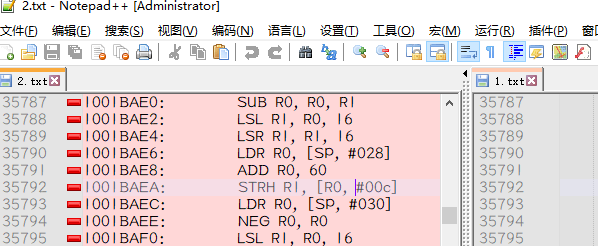
设置为次要对比项，

稍等片刻就会显示出两者的差异，

不用管1.txt，只是为了让2.txt高亮，

在2.txt标签里Ctrl+F搜索 1001BAEA

只有唯一一条，并且在红色区域内，



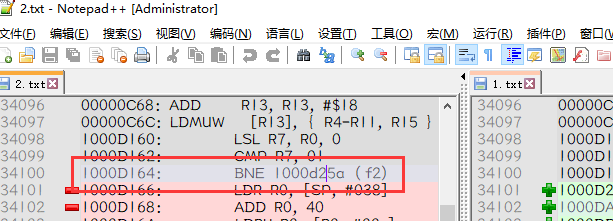
这时候在1.txt内容里点一下，就会跳到与2.txt同一内容区块，

可以看到2.txt里的红色区域文字在1.txt里是不存在的，

若是尝试在1.txt里搜索 1001BAEA，是绝对搜索不到的，

能懂什么意思吧，因为1.txt导出的是未击中的指令，

在2.txt的扣血指令地址往上找，



可以看到是 1000D164 这个跳转让2.txt里出现了1.txt没有的内容，

记录 1000D164 这个地址，在调试器里键入 bp 1000D164

然后对着空气攻击一下，



游戏会立即中断，在调试器里会出现指令，

在这个指令上回车单步执行，会发现必定跳转，因为没击中敌方，

但这个指令地址也可能不是是否攻击到的跳转，

那就来试验下，后面的D179是字节操作码，

键入 maincpu.rw@1000D164=0000

将D179改为0000，就相当于nop掉了这一句，

也就是不会再跳转，



这时候再对空气攻击，会发现敌方被全屏攻击了

道具及其它攻击也是同样的方法改，

把攻击落空必定跳转改成必定不跳转，

把攻击落空必定不跳转改成必定跳转

需要注意的是若还没攻击就立刻断下的地址在大部分游戏里绝不会是是否攻击到的判断

其次，尽可能的减少影响因素，最简单直白的意思就是让敌方数量尽可能的只有1个，

若是一堆小怪那还改个球，文件大小动不动几百M

理论上大部分游戏都可以这样修改全攻，

也有些可能要改一堆的连续跳转才能实现理想的全攻